MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2017/2018

TSN3251 – COMPUTER SECURITY

(All Sections / Groups)

17 March 2018
9:00 a.m. – 11:00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This paper consists of 6 pages (including cover page) with 5 Questions only.
2. Attempt **ALL FIVE** questions. The distribution of the marks for each question is given. This paper carries **100 marks**.
3. Please print all your answers in the Answer Booklet provided.

Question 1 (20 Marks)

a) Confidentiality, integrity and availability (CIA), is a model designed to guide policies for information security within an organization. Explain and give an example each on what is meant by the THREE (3) terms: **confidentiality**, **integrity** and **availability**.

[6 marks]

b) In terms of computer security, distinguish between the terms "vulnerability", "threat" and "control".

[3 marks]

c) Explain the following principles in computer security.

(i) Principle of Adequate Protection
(ii) Principle of Easiest Penetration
(iii)Principle of Effectiveness

[3 marks]

d) If plaintext is denoted by P, ciphertext is denoted by C, the encryption function is denoted by E( ) and the encryption key is denoted by K_s, write down the formal notation relating plaintext and ciphertext.

[2 marks]

e) Julius Caesar invented the Caesar Cipher, which is a form of substitution encryption.

(i) Briefly explain what is substitution cipher and how it works.

[1 mark]

(ii) Decrypt the following message that was encrypted using a left rotation of three places. Do show your encryption/decryption table.

VDZDGHNUDE

[2 marks]

Continued ...

(iii)Explain how can Frequency Analysis be used to conduct cryptanalysis on substitution cipher.

[3 marks]

Question 2 (20 Marks)

a) Decrypt the following message that was encrypted using the Playfair cipher with the key "jingga". Ensure that you show each decrypting step clearly.

LTBGEMAPSYROMG

[8 marks]

b) Given the following 2 by 2 matrix, $\begin{bmatrix} 1 & 5 \\ 3 & 4 \end{bmatrix}$, compute the inverse of the matrix in modulo 26 arithmetic.

$$\begin{bmatrix} 1 & 5 \\ 3 & 4 \end{bmatrix}^{-1}$$

[8 marks]

c) Decrypt the following text that was encrypted using a 3 row rail fence cipher.

TIUAANHSSFNXMNTOIAEII

[4 marks]

Question 3 (20 Marks)

a) Given the input 101001 and using the S-Box provided below, what is the binary output of the S-Box?

	S[1]															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

[3 marks]

Continued ...

b) Euler's Theorem is a generalization of the Fermat's theorem. It is stated as

$$a^{\varphi(n)} \bmod n = 1, \text{ where } \gcd(a,n)=1$$

Show how you can solve $7^{503} \bmod 12$ using the Euler's Theorem (hint: you need some help from the square and multiply rule).

[8 marks]

c) RSA is the best known and most widely used algorithm for Public Key Cryptography. Describe the steps for RSA Key Generation.

[4 marks]

d) Miller Rabin Algorithm is a primality test based on the Fermat's Theorem. The algorithm is as described below.

The test for (n) is:

1. Find integers k, q such that $k > 0$, q is an odd number, so that $(n-1)=2^k q$
2. Select a random integer a, where $1 < a < n-1$
3. if $a^q \bmod n = 1$ then return ("maybe prime");
4. for $j = 0$ to $k - 1$ do
    5. if $(a^{2^j q} \bmod n = n-1)$
        then return("maybe prime")
6. return ("composite")

The algorithm above does not ever return a "prime". Explain why the algorithm does not return "prime".

[2 marks]

e) Both Message authentication codes (MAC) and digital signatures are used to authenticate the content of a message. State a major difference between MAC and digital signatures?

[3 marks]

Continued ...

Question 4 (20 Marks)

a) State what is meant by the following FOUR (4) software threats.

- Virus
- Worms
- Trap Doors
- Trojan Horse

[4 marks]

b) In the design of an anti-virus system, explain, with the aid of diagrams, the SEVEN steps of how the IBM Digital Immune System works.

[4 marks]

c) Programmers do make errors that can cause program malfunctions and a few classes of errors have plagued programmers and security professionals for decades. Three (3) classic error types that have enabled many security breaches are

(i) Buffer Overflows,

(ii) Incomplete Mediation, and

(iii) Time-of-Check to Time-of-Use Errors.

Explain each of the three (3) types mentioned above and also state how they can be prevented or mitigated.

[6 marks]

d) Give an overview of Database SQL Injection attack and explain technically how it works. Use code snippets to explain.

[6 marks]

Continued ...

Question 5 (20 Marks)

a) State and discuss any TWO (2) advantages and TWO (2) disadvantages of using biometrics as a method of authentication.

[4 marks]

b) Write a pseudo code for a program to conduct brute force (exhaustive) attack on an encrypted password. Assume that the password was encrypted using a one-way encryption algorithm (such as SHA-512 or MD5). You do not need to mention specific program names, just a pseudo code to show your understanding of how a brute force attack is done. For simplicity, you can assume that the password is of only 3 characters long.

[4 marks]

c) What is meant by a two-factor authentication and give an example of it by explaining which of the two-factors can be used.

[2 marks]

d) Network Based Intrusion Detection Systems (IDS) are generally implemented in stealth mode. Give a detailed explanation what this means and how does it work (use a diagram to illustrate).

[4 marks]

e) Explain the workings of each of the following three (3) Denial of Service (DOS) attacks:-

(i) Ping of Death

(ii) Smurf

(iii)SYN Flooding

[6 marks]

END OF EXAM PAPER